UNITED STATES DISTRICT COURT
DISTRICT OF NORTH DAKOTA

Jason Quaife, John Hoffer, Amanda Koffler, and Alec R. Kiesow, on behalf of themselves individually and all others similarly situated, Plaintiffs, v. Brady, Martz & Associates, P.C., Defendant.	Case No. 3:23-cv-176-PDW-ARS **PLAINTIFFS' MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS**

INTRODUCTION

In the course of its financial-services business, Defendant Brady, Martz & Associates, P.C., ("Defendant") collects and stores sensitive data belonging to its customers, and it is responsible for securing and protecting that data. Defendant failed to do so and negligently allowed its systems to be breached and its customers' data to be exfiltrated. This failure allowed Plaintiffs' sensitive and personal information to fall into the hands of cybercriminals to be exposed, sold on the dark web, and/or used in any number of other malicious ways.

Defendant's attempt to absolve itself of its responsibility for the Data Breach is unavailing. Plaintiffs have adequately alleged that Defendant was negligent, that it violated state statutes, and that it was unjustly enriched by its acts and omissions. Plaintiffs have standing to pursue the relief they seek to redress the harms caused by Defendant's conduct. Defendant's motion to dismiss should accordingly be denied.

STATEMENT OF FACTS

This case stems from a security breach of Defendant's systems caused by an unknown

third-party threat actor. (Consolidated Amended Complaint ("CAC"), ECF No. 15 at ¶ 4). Defendant is a sophisticated accounting and audit services company that provides financial services for a wide range of industries, including agribusiness, communication & electric utilities, construction & real estate, dealerships, financial institutions, government, healthcare, nonprofit, oil & gas, and tribal gaming (CAC at ¶ 2), in the process collecting the personally-identifying information ("PII") and private health information ("PHI") (collectively, "PI") of individuals who have relationships with those companies. (CAC at ¶ 3). On November 19, 2022, Defendant discovered the security breach, but it did not begin notifying affected individuals until September 8, 2023. (CAC at ¶ 4). As a result of the data breach, Plaintiffs and putative class members suffered damages as outlined in the CAC. (CAC at ¶¶ 72, 74–77, 83–84, 88–89, 91–93, 99, 101–104, 109–111, 113–115). Plaintiffs allege claims for negligence (CAC ¶¶ 133–153), negligence *per se* (CAC ¶¶ 154–161), unjust enrichment (CAC ¶¶ 162–174), declaratory judgement (CAC ¶¶ 175–180), violation of the Massachusetts Consumer Protection Act (CAC ¶¶ 181–185), and violation of the North Dakota Business Records Disclosure Act (CAC ¶¶ 186–191).

LEGAL STANDARD

On a motion to dismiss, courts must accept the allegations as true and draw all reasonable inferences in the plaintiffs' favor. *Stodghill v. Wellston Sch. Dist.*, 512 F.3d 472, 476 (8th Cir. 2008). A plaintiff must allege "enough facts to state a claim to relief that is plausible on its face."[1] *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). This standard "do[es] not require heightened fact pleading of specifics." *Id.* A court should construe a complaint liberally and in the light most

[1] Although Plaintiffs raise state law claims in addition to their federal challenges, the Eighth Circuit has stated: "We apply federal pleading standards—Rules 8 and 12(b)(6)—to the state substantive law to determine if a complaint makes out a claim under state law." *See Karnatcheva v. JPMorgan Chase Bank, N.A.*, 704 F.3d 545, 548 (8th Cir. 2013).

favorable to the plaintiff. *See Luney v. SGS Auto. Servs., Inc.*, 432 F.3d 866, 867 (8th Cir. 2005). "While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions." *Eckert v. Titan Tire Corp.*, 514 F.3d 801, 806 (8th Cir. 2008) (quoting *Twombly*, 550 U.S. at 544).

ARGUMENT

I. Plaintiffs have plausibly pleaded their negligence claims.

In its attempt to assert it did not owe a duty to Plaintiffs, Defendant tries to define the scope of a duty under the principles of negligence extremely narrowly, avoiding several of Plaintiffs' allegations that assert basic common law duties not associated with statutes or special relationships. Defendant argues that it had no duty to provide adequate security to protect Plaintiffs' sensitive PI because it is not clear Plaintiffs entrusted this information to Defendant, the statutory duties alleged do not create a duty under a negligence cause of action, and because there was no special relationship between the parties. (Def.'s Memo. of Law, ECF No. 19 at 4–6 (hereinafter, "Memo.")). Plaintiffs do not allege Defendant owed a duty to protect them from crime, but rather owed a duty to everyone concerned to employ reasonable data security due to the foreseeable risk that the highly sensitive PI would be targeted by data thieves. Because Plaintiffs allege cognizable duties, Defendant's motion should be denied.

A. Defendant owed plaintiffs a common law and statutory duty of care.

Under North Dakota law, a defendant owes a duty "to exercise ordinary care and skill in its undertaking [] for the protection of persons who foreseeably or with reasonable anticipation may have been injured by its failure to do so." *Layman v. Braunschweigische Maschinenbauanstalt, Inc.*, 343 N.W.2d 334, 341 (N.D. 1983). "The duty exists independent of

the contract, and privity of contract is not required." *Id.* Whether a duty exists is a question of law, "but if the duty depends on the foreseeability of injury, the question is to be left to the fact finder unless the issue is such that reasonable men could not differ." *North Dakota v. United States*, Case No. 1:19-cv-00150, 2023 WL 8627630, at *4 (D.N.D. Dec. 13, 2023) (citing *Kirton v. Williams Elec. Co-op., Inc.*, 265 N.W.2d 702, 704 (N.D. 1978)); *accord Decker v. I.E. Miller Servs., Inc.*, Civil No. 4:14-cv-88, 2017 WL 10316143, at *3 (D.N.D. Mar. 3, 2017) (determining that a duty to exercise reasonable care exists). Under a negligence theory of liability, a "duty extends to those injuries that are foreseeable." *Nelson v. Gillette*, 571 N.W.2d 332, 340 (1997). Plaintiffs have pleaded that their damages were a direct, proximate, and foreseeable result of Defendant's negligence. (CAC at ¶¶ 6, 30, 142, 145, 148(a), 153, 189).

While Plaintiffs are not aware of any cases applying this principle to a data breach in North Dakota, other courts have applied similar formulations of a common law duty in similar circumstances and found that a duty exists. *See, e.g., In re: Netgain Tech., LLC*, 21-CV-1210 (SRN/LIB), 2022 WL 1810606, at *11 (D. Minn. June 2, 2022) ("Plaintiffs contend that this is not a special relationship case, but rather a general negligence case where Netgain's own conduct, in failing to maintain appropriate data security measures, created a foreseeable risk of the harm that occurred, and Plaintiffs were the foreseeable victims of that harm. The Court agrees with Plaintiffs."); *In re Blackbaud, Inc., Customer Data Breach Litig.*, 567 F. Supp. 3d 667, 682 (D.S.C. 2021) ("A common law duty may arise where a defendant creates a situation that [it] knew or should have known posed a substantial risk of injury to a plaintiff." (internal quotation omitted)).

Courts have repeatedly found a legal duty for merchants to protect consumers confidential and sensitive information entrusted to its possession; there need not be any special relationship. *See Auer v. Trans Union LLC*, No. 4:14-CV-125, 2015 WL 11393824, at *5 (D.N.D. Apr. 7, 2015),

vacated and remanded on other grounds by Auer v. Trans Union, LLC, 902 F.3d 873 (8th Cir. 2018) ("Federal regulations require any person 'who maintains or otherwise possesses consumer information for a business purpose [to] properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."); *see also, In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1310 (D. Minn. 2014) ("Plaintiffs have plausibly alleged that Target's actions and inactions—disabling certain security features and failing to heed the warning signs as the hackers' attack began—caused foreseeable harm to Plaintiffs.") Several courts have also found a common law duty to act reasonably with respect to data security. *See, e.g.*, *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 529–30 (M.D. Pa. 2021) ("Based on Plaintiffs' allegations, we find that Defendant's affirmative act of retaining credit and debit card information which created a risk of foreseeable harm from unscrupulous third parties is enough to recognize a legal duty here."); *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 400 (E.D. Va. 2020) (finding duty to protect PI based on voluntary undertaking doctrine); *Portier v. NEO Tech. Sols.*, 3:17-CV-30111-TSH, 2019 WL 7946103, at *13 (D. Mass. Dec. 31, 2019), report and recommendation adopted, 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *Castillo v. Seagate Tech., LLC*, No. 16-CV-01958-RS, 2016 WL 9280242, at *3 (N.D. Cal. Sept. 14, 2016) (holding under California law, the defendant "was duty-bound to take reasonable steps to protect all personal identifying information it obtained from its employees, including information pertaining to employees' spouses and dependents"); *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1363 (S.D. Fla. 2015) (holding that ambulance service had a duty to exercise reasonable care in safeguarding and protecting the plaintiff's sensitive information).

In addition to a common law duty of care, North Dakota has also codified Defendant's general duty of care under N.D.C.C. § 9-10-01, which states that "[e]very person is bound without contract to abstain from injuring the person or property of another or infringing upon any of the person's rights." *Berger v. Sellers*, 996 N.W.2d 329, 346 (N.D. 2003) (recognizing a statutory general duty of care).[2] "A person is responsible . . . for an injury occasioned to another by the person's want of ordinary care or skill in the management of the person's property or self." N.D.C.C. § 9-10-06. Thus, under North Dakota law, every person has a duty to act reasonably to protect others from harm. *Wood v. City of Bismarck*, No. 1:21-cv-00063, 2023 WL 4044513, at *8 (D.N.D. May 17, 2023).

Plaintiffs allege a duty to employ reasonable data security and to take other actions protecting the sensitive PI that was obtained in the course of providing services to vendors. (CAC at ¶¶ 136–37, 147).[3] Plaintiffs further allege that Defendant owed a duty to everyone concerned to employ reasonable data security due to the foreseeable risk that the highly sensitive PI would be targeted by data thieves. (*Id.* at ¶¶ 5, 27–29, 33, 42). The common law duty to safeguard information is properly alleged which also aligns with North Dakota statutory principles and serves as a sufficient basis for Plaintiff's establishment of duty as an element of negligence. Defendant's motion should therefore be denied.

B. There is a sufficient relationship between the parties to establish a duty.

[2] "Statutory principles govern over general common law if there is a conflict." *See Martin v. Rath*, 589 N.W.2d 896, 901 (N.D. 1999).

[3] Despite Defendant's privacy policy proclaiming that it "is committed to maintaining the privacy of information *related to its clients, customers and consumers* that it collects and maintains as a result of its business practice," Defendant now claims it has no such duty. (CAC at ¶ 21 (emphasis added)). Defendant likely does not use its current opportune defense—that a duty, "in reality, d[oes] not exist" to protect sensitive personal information—as a sales pitch to its customers. (Memo. at 4–5).

Defendant also asserts that the relationship between the parties is at such a distance as to preclude a finding of a duty from the defendant to Plaintiffs. (Memo. at 5). But courts have found that similar relationships between parties support a finding of a duty. In *In re: Netgain Tech., LLC*, 2022 WL 1810606 at * 9 (D. Minn. June 2, 2022), the court rejected a similar argument where a third-party information technology and cybersecurity service provider suffered a data breach. The court cited *Castillo*, where an employer was found to have a duty to protect personal information of non-employees on the basis that the information was entrusted to it, not on the fact that it was the plaintiffs personally entrusting the defendant with the information. *Id.* (citing 2016 WL 9280242, at *3 ("In *Castillo*, a California district court found that an employer had a duty to protect the personal information it possessed regarding the spouses and dependents of its employees and former employees, despite no privity of contract with those persons.")). Even though there may not be direct relationship between the parties, the fact that the defendant was in possession of the valuable property of the plaintiff establishes the relationship sufficiently to create a duty. Here too, Defendant's argument should fail.

C. The FTCA serves as an alternative basis for establishing the requisite duty.

A duty is imposed as a result of willful acts for an injury. Under North Dakota law the violation of a statutory duty is evidence of negligence. *Larson v. Kubisiak*, 558 N.W. 852, 854–55 (N.D. 1997). Courts have held that Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), "is a statute that creates enforceable duties" and those duties are applicable to data breach cases "based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context." *In re Marriott Int'l, Inc., Cust. Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 481 (D. Md. 2020); *see also In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *8 (N.D. Ga. Mar. 5, 2018) (noting that several courts have held

that Section 5 of the FTC Act can serve as a basis for a negligence per se claim in the data breach setting).[4]

Under Minnesota law,[5] it is clear in the data breach context under the FTCA that "negligence per se may exist when the reasonable person standard is supplanted by a standard of care established by the legislature." *Perry v. Bay & Bay Transp. Servs., Inc.*, 650 F. Supp. 3d 743, 755 (D. Minn. 2023) (citing *Seim v. Garavalia*, 306 N.W.2d 806, 810 (Minn. 1981)); *accord Gradjelick v. Hance*, 646 N.W.2d 225, 234 (Minn. 2002) (finding that under Minnesota law negligence per se exists for statutory violations). Here, the FTCA provides an alternative basis by which to define Defendant's duty and breach of that duty as alleged in Count II.

II. Plaintiffs have plausibly pleaded their unjust enrichment claims.

The North Dakota Supreme Court describes unjust enrichment claim as "a broad, equitable doctrine . . . to prevent a person from unjustly enriching himself at the expense of another." *Hayden v. Medcenter One, Inc.*, 828 N.W.2d 775, 781 (N.D. 2013). Unjust enrichment "may be invoked when a person has and retains money or benefits which in justice and equity belong to another." *Ritter, Laber and Assoc., Inc. v. Koch Oil, Inc.*, 680 N.W.2d 634, 642 (N.D. 2004).

---

[4] Several other courts have declined to dismiss negligence *per se* claims at the pleading stage in data breach cases. *E.g.*, *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 760–61 (C.D. Ill. 2020); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019); *In re Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *14 (N.D. Ga. Mar. 5, 2018); *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, MDL 2583, 2016 WL 2897520, at *4 (N.D. Ga. May 17, 2016); *First Choice Fed. Credit Union v. Wendy's Co.*, No. 16-506, 2017 WL 9487086, at *4 (W.D. Pa. Feb. 13, 2017).

[5] A choice of law analysis for the Minnesota Plaintiffs Quaife, Kiesow, and Stock allow for a negligence per se claim as a separate count under Minnesota law. *Kraft v. Essentia Health*, 602 F. Supp. 3d 1130, 1140 (D.N.D. 2022) (analyzing a peer review privilege choice of law between North Dakota and Minnesota). Although Defendant's principal place of business is located in Grand Forks, North Dakota, it also operates throughout northwestern Minnesota. (*See* CAC at ¶ 1).

To recover under a theory of unjust enrichment, the plaintiff must prove: (1) an enrichment, (2) an impoverishment, (3) a connection between the enrichment and the impoverishment, (4) the absence of a justification for the enrichment and impoverishment, and (5) the absence of a remedy provided by law. *McColl Farms, LLC v. Pflaum*, 837 N.W.2d 359, 367 (N.D. 2013) (citation omitted). Defendant challenges the connection between the parties, Plaintiff's loss, and the relief to which Plaintiffs and Class members are entitled. Because Defendant is wrong on all arguments, the Court should sustain Plaintiffs' claim.

A. Defendant was enriched at Plaintiffs' expense.

Defendant contends that Plaintiffs' claim for unjust enrichment fails because there is no direct relationship between Plaintiffs and Defendant, as Defendant contract with Plaintiffs' employers and not Plaintiffs themselves. (Memo. at 7). Thus, under Defendant's view, Plaintiffs must allege a direct, monetary nexus between the enriched party and impoverished party. This is incorrect.

First, North Dakota does not require that there be a direct relationship between the plaintiff and defendant. Indeed, Defendant cites no authority for its argument, because precedent is not on its side. For example, in *McDougall v. AgCountry Farm Credit Servs.*, 960 N.W.2d 792 (N.D. 2021), the North Dakota Supreme Court affirmed the trial court's finding of unjust enrichment where the plaintiffs transferred property to their son, based on representation that the defendant made to the plaintiffs' son. *Id.* at 798–99. The lack of a direct relationship between plaintiff and defendant did not preclude the claim for unjust enrichment. *Id.* at 799 (holding that if a "third party has participated somehow in the transaction through which the benefit is obtained, that fact must be considered by the court" (quoting *Midland Diesel Serv. & Engine Co. v. Sivertson*, 307 N.W.2d 555, 558 (N.D. 1981))). Thus, it is not required that Plaintiffs have a direct relationship with

Defendant. Instead, it is sufficient that Plaintiffs provided their PI to their employers, who had a contractual relationship with Defendant.

Defendant's second argument is that Plaintiffs did not suffer any monetary loss. But, contrary to Defendant's assertion, unjust enrichment may lie even when the benefit received or loss suffered is not a monetary benefit. *See, e.g.*, *Id.* (sustaining unjust enrichment claim where plaintiffs deprived of real property). Indeed, the Eighth Circuit Court of Appeals has held that "benefit" can denote "any form of advantage" beyond financial or monetary concerns. *See CRST Expedited, Inc. v. TransAm Trucking, Inc.*, 960 F.3d 499, 508 (8th Cir. 2020) ("Benefits can be direct or indirect, and can involve benefits conferred by third parties." (quotation omitted)).

Here, Defendant received a benefit from its use of Plaintiffs' and Class members' PI, in the money and time Defendant saved by failing to implement adequate data security practice and procedures, and in the form of money paid to Defendant for services that it would not have obtained had it disclosed that had inadequate data security practices. (*See* CAC ¶¶ 71, 98, 108, 163–169). Plaintiffs and Class members reasonably expected that Defendant would comply with its obligations to protect their PI. (CAC ¶ 28). Plaintiffs and Class members suffered impoverishments in the diminished value of their PI, the increased likelihood of identity theft, and the time and effort that Plaintiffs had to expend to mitigate the effects of the data breach. (CAC ¶¶ 46–70, 72, 83, 89, 99, 109, 170). Those allegations are sufficient to meet the enrichment, impoverishment, and unjust retention of benefit elements. *See Baldwin v. Nat'l Western Life Ins. Co.*, No. 2:21-CV-04066-WJE, 2021 WL 4206736, *8 (W.D. Mo. Sept. 15, 2021) (stating that

courts within the Eighth Circuit permit unjust enrichment claims in data breach actions (citing *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014)).[6]

B. Plaintiffs' alleged theory of relief is proper.

Defendant misconstrues the allegations in the complaint, creating a strawman to argue that Plaintiffs theory of recovery is improper. Damages for unjust enrichment may be measured as "the defendant's enrichment or the value of the benefit [the defendant] received." *KLE Const., LLC v. Twalker Devel., LLC*, 887 N.W.2d 536, 540 (N.D. 2016).[7] Contrary to Defendant's assertion, the CAC, in fact, alleges that Plaintiffs and Class Members are entitled to the value of the proceeds that Defendant unjust received from its failure to implement adequately protect Plaintiffs' and Class members PI. (*See* CAC at ¶ 173–174). Indeed, the CAC requests that "Defendant [] be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful and inequitable proceeds it received . . . ." (CAC at ¶ 174). Defendant ignores these allegations. The mere fact that Plaintiffs also allege that they were damaged from the diminished value of their PI does not negate the fact that Plaintiffs request "recovery . . . measured by the benefit to the defendant." *See KLE Const.*, 887 N.W.2d at 540 (citations omitted). As such, the Court should deny Defendant's motion.

III. Plaintiffs have standing to seek declaratory and injunctive relief.

[6] Defendant incorrectly contends that the unjust enrichment claim fails because Plaintiffs fail to allege that Defendant did not perform tax and accounting services. (Memo. at 8 n.2). Yet no such allegation is required. Plaintiffs need only allege that defendant was unjustly enriched because they would not have provided their PI to Defendant, or Defendant would not have been able to shirk its data security responsibilities. *See In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014); *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1145 (C.D. Cal. 2021).

[7] Defendant mis-attributes the foregoing quote to *Ritter, Laber and Assocs., Inc. v. Koch Oil, Inc.*, 680 N.W.2d 634.

Defendant argues that Plaintiffs' claims for declaratory judgment and injunctive relief should be dismissed because Plaintiffs "have not suffered an injury in fact" and therefore do not have standing to bring such claims. (Memo. at 9).

"A plaintiff has suffered an injury-in-fact if he has experienced an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical." *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 908 (8th Cir. 2016) (quotation omitted). To "pursue forward-looking, injunctive relief to prevent" future harm, a plaintiff must allege that the "risk of harm is sufficiently imminent and substantial." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210 (2021). Courts have nearly universally held that data breaches involving PI create a substantial risk of future harm. *See In re: Netgain Tech., LLC*, 2022 WL 1810606, at *5 (collecting cases).

Defendant cites only two district court cases to support its opposite conclusion, and both are highly distinguishable. In *In re Pawn America Consumer Data Breach Litigation*, the district court concluded that plaintiffs had not alleged a sufficiently imminent risk because they "allege[d] *only* that they have an interest in ensuring that their private information, which is believed to remain in the possession of Pawn America, is protected from further breaches." No. 21-cv-2554 (PJS/JFD), 2022 WL 3159874, at *3 (D. Minn. Aug. 8, 2022) (emphasis added). Likewise, in *Hall v. Centerspace, LP*, the plaintiffs alleged only that they suffered "continued risk to their PII." 22-cv-2028 (KMM/DJF), 2023 WL 3435100, at *2 (D. Minn. May 12, 2023). Here, Plaintiffs allege far more.

Plaintiffs thoroughly allege that cyberattacks and data breaches have been growing increasingly common for years, that Defendant knew or should have known of this increased risk, and that it nevertheless maintained inadequate security measures. (CAC at ¶¶ 29–33, 79).

Defendant's laissez-faire cybersecurity practices in light of such risks, as Plaintiffs allege, makes the threat of future attacks and theft of their PI imminently likely. (CAC at ¶¶ 63, 149, 179). Contrary to Defendant's claim, Plaintiffs do not merely allege a continuing interest in protecting their information. Indeed, Plaintiffs seek a declaration that Defendant's existing security measures are inadequate because it has failed to specify what measures, if any, have been taken to prevent future breaches. (CAC at ¶ 180). These allegations are sufficient at the motion-to-dismiss stage.

Defendant's extraordinarily broad claim that "[d]istrict courts in the Eighth Circuit . . . do not permit such 'forward looking' claims in data breach cases" is simply incorrect. (Memo. at 10). In *Perry v. Bay & Bay Transportation Services, Inc*., the court found that Plaintiffs had standing to pursue injunctive relief "to require [defendant] to implement certain data security measures" because the plaintiffs plausibly alleged an increased risk of future identify theft. 650 F. Supp. 3d 743, 747, 751–52 (D. Minn. 2023). In *In re: Netgain Technology, LLC*, the district court found that the plaintiffs' allegations that the defendant "continues to provide inadequate and unreasonable data security, and that they and the Class continue to suffer injury" was sufficient to for a declaratory judgment claim to survive a motion to dismiss. 2022 WL 1810606, at *16–17 (quotations omitted). Other district courts in this circuit have followed suit. *E.g.*, *Weisenberger v. Ameritas Mut. Holding Co*., 597 F. Supp. 3d 1351, 1359 (D. Neb. 2022) (holding that plaintiffs adequately alleged future risk of harm because of "the sensitive nature of the PII compromised, and the allegations that the plaintiff's PII will be made available on the dark web"); *Coffey v. OK Foods Inc.*, No. 2:21-CV-02200, 2022 WL 738072, at *3 (W.D. Ark. Mar. 10, 2022) (concluding that plaintiff adequately alleged imminent future injury because she alleged that her name and social security number were stolen in a data breach); *Mackey v. Belden, Inc.*, No. 4:21-CV-00149-JAR, 2021 WL 3363174, at *12 (E.D. Mo. Aug. 3, 2021) (declining to dismiss claim for injunctive

relief because the plaintiff "alleged that her PII remains in Belden's possession and at risk of further disclosure" if such relief is denied). Defendant's motion should likewise be denied.

IV. Plaintiffs have adequately pleaded claims under the MCPA.

Defendant does not attack the main thrust of the Massachusetts Consumer Protection Act, conceding that Plaintiff Hoffer's claim that Defendant's actions constitute "deceptive acts or practices in the conduct of any trade or commerce" under the definition of the MCPA. Instead, Defendant states that Plaintiff's "MCPA claim fails because it is not based on unfair or deceptive practices that 'occurred primarily and substantially within the commonwealth [of Massachusetts].'" (Memo. at 11 (citations omitted)). However, Defendant ignores both binding precedent and the following sentences of the MCPA in making this argument. The very next sentence in Mass. Gen. Laws ch. 93A § 11 states, "For the purposes of this paragraph, the burden of proof shall be upon the person claiming that such transactions and actions did not occur primarily and substantially within the commonwealth." Defendant makes no such showing, arguing merely that Plaintiff's allegations do not support an inference sufficient to meet the MCPA. (Memo. at 11). This alone is insufficient to sustain Defendant's motion.

However, even putting that aside, there is a three-factor test to determine the applicability of the MCPA: "(1) where the alleged conduct took place, (2) where the plaintiff received and acted upon the statements, and (3) where the plaintiff's losses were suffered." *Bradley v. Dean Witter Realty, Inc.*, 967 F. Supp. 19, 29 (D. Mass. 1997) (citing *Bushkin Assoc., Inc. v. Raytheon Co.*, 473 N.E.2d 662, 672 (Mass. 1985)). The conduct in question likely took place in North Dakota, as Defendant's employees and decision-makers are (as far as Plaintiffs know) all in North Dakota. However, the second and third factors both weigh in favor of Plaintiff. Defendant cannot and does not seriously contest that Plaintiff received and acted upon Defendant's statements (including

those in the notice letter) in Massachusetts. Plaintiff received the notice letter at his Massachusetts address and made all efforts to remediate the damage done by the Data Breach in Massachusetts– as would have all members of the Massachusetts subclass. As such, the balance of the test is in favor of Massachusetts, not North Dakota.

Next, Defendant argues that Plaintiff has not adequately pleaded that Defendant *caused* Plaintiff's loss. However, in doing so, Defendant misstates that causation at issue, conflating the fact that Plaintiff does not know how Defendant came into possession of his personal information with the erroneous idea that Defendant may not have had Plaintiff's personal information at all:

> Yet Plaintiff Hoffer cannot be heard to complain Defendant's conduct caused him losses. Contrary to the CCAC's conclusory allegations of deception and unfair practices perpetrated against Plaintiffs, Mr. Hoffer admits he is "uncertain of exactly how Defendant" came to have his information and he has "never" directly used Defendant's accounting, tax, or any other service.

(Memo. at 12). Defendant does not argue that it did not have Plaintiff's personal information. Indeed, Plaintiff's well-pleaded allegations indicate that Plaintiff received a letter from Defendant indicating that it did have Plaintiff's personal information and that that information was stolen. (CAC at ¶¶ 4, 81). Further, Plaintiffs have pleaded that Defendant is an accounting and audit services firm who routinely works for businesses and receives the personal information of individuals, such as Plaintiff, from those companies. (CAC at ¶¶ 2–3). It is not necessary at this stage to know from which company Defendant received Plaintiff's information to know that, in fact, it was received by Defendant. In making its argument, Defendant attempts to blur the meaning of causation in a way designed to mislead as to whether it actual had the information in question.

Defendant's one supporting case to this argument is *In re: TJX Companies Retail Sec. Breach Litigation,* in which the court examined the role of a class of putative banks (not

individuals) who sought damages from defendants TJX and Fifth Third as a result of a data breach at TJX. In that case, the court held that

> it will not be enough for the banks to simply show that the data breach is the but-for cause of their loss or that TJX and Fifth Third failed to remedy shortcomings in its data security systems. They will have to show that, had TJX and Fifth Third been candid about their data security compliance, their losses would not have occurred.

In re: TJX Companies Retail Sec. Breach Litigation, 246 F.R.D. 389, 398 (D. Mass. 2007). Plaintiff has adequately made that showing here, arguing that Plaintiff's information was in Defendant's hands (as discussed *supra*), and that Plaintiff had to take efforts to remediate the breach (CAC ¶¶ 83–85). Further, as a class certification decision, *TJX* examined whether reliance would need to be shown across all members of the class, a step this Court is not yet needed to examine. Accordingly, the argument as to whether or not different policies on the part of Defendant could have made a difference is not required at this stage.

V. Plaintiffs have plausibly pleaded claims under N.D.C.C. § 51-22-02.

To manufacture a heightened standard of liability, Defendant speciously asserts that "N.D. Cent. Code § 51-22-02 governs *intentional* disclosures by business entities, not nonconsensual theft by cyberthieves." (Memo. at 13 (emphasis added)). Defendant seeks to turn a straight-forward state statutory analysis into an entangled semantics exercise. (*See id*. at 13–15). According to Defendant, liability under the statute only attaches "when a business *willfully* discloses information." (*Id.* at 14 (emphasis added)). Defendant's attempt to insert unintended intentional or willful text into a North Dakota statute fails.

The North Dakota statute that Plaintiffs have pleaded prohibits the disclosure of information, and states that:

> No business entity which charges a fee for data processing services performed may disclose in whole or in part the contents of any record, including the disclosure of information contained in the record through inclusion in any composite of

> information, which is prepared or maintained by such business entity to any person, other than the individual or business entity which is the subject of the record, without the express written consent of such individual or business entity.

N.D.C.C. § 51-22-02(1).

First, if the state legislature had intended for the "disclosure" to include an affirmative intentional or willful act, it would have specifically drafted the statute to include an intentional disclosure as it has elsewhere in the North Dakota Century Code for similar statutes.[8] Indeed, a court should "not add words or additional meaning to a statute." *Larsen v. North Dakota Dept. of Transp.*, 693 N.W.2d 39, 43 (N.D. 2005) (refusing to "add words or phrases which the legislature did not include," declining to "rewrite the statute"). "The legislature's silence . . . is a strong indication it did not intend such a remedy." *Ernst v. Brudick*, 687 N.W.2d 473, 478 (N.D. 2004) (citation omitted); *accord Public Servs. Comm'n v. Wimbledon Grain Co.*, 663 N.W.2d 186, 196 (N.D. 2003) (explaining that the court "will not correct an alleged legislative 'oversight' by rewriting unambiguous statutes to cover the situation at hand"). Moreover, "[c]ourts are to presume the legislature said all that it intended to say." *In re Racing Servs., Inc.*, 504 B.R. 549, 554 (D.N.D. 2014) (citation omitted) (determining that "[w]ords or phrases cannot be added by a court"). Statutes may also be read in relation to other statutes involving the same or similar subject matter to discern legislative intent. *Trade 'N Post, LLC v. World Duty Free Americas, Inc.*, 628 N.W.2d 707, 711 (N.D. 2001); *see also PHI Fin. Servs., Inc. v. Johnston Law Office, P.C.*, 937 N.W.2d 885, 889 (N.D. 2020) (recognizing that statutes should be construed in a "practical manner, giving

[8] The North Dakota legislature has consistently included the term "intentional" when it was meant for a necessary willful or intentional act of "disclosure." *See* N.D.C.C. § 32-49-02 (stating an "individual who is identifiable and who suffers harm from a person's *intentional disclosure* or threatened disclosure of an intimate image that was private without the depicted individual's consent has a cause of action" (emphasis added)); N.D.C.C. § 6-08.1-08 (stating that a "person is liable to the customer for *intentional* violations of this chapter" and liable for "[a]ctual damages caused by the *disclosure* of the customer information" (emphasis added)).

consideration to the context of the statutes and the purpose for which they were enacted"). Clearly, the North Dakota Legislature is fully aware of how to draft an affirmative intentional disclosure statutory requirement, if that was indeed its intent. *Carlson v. Roetzel & Andress*, No. 3:07-cv-33, 2008 WL 873647, at *8 (D.N.D. Mar. 27, 2008) (recognizing that "the legislature did not intend to create [causes of action] by implication"); *see supra* note 9.

Second, as Defendant points out, N.D.C.C. § 51-22 does not defined "disclose" or "disclosure," but the statutory definition of these exact terms from similar statutes elsewhere in the North Dakota Century Code applies directly to the prohibition of disclosure of an individual's personal records under N.D.C.C. § 51-22-02. The North Dakota Supreme Court has held that "[w]hen the meaning of a word or phrase is defined in a section of our Code, *that definition applies to any use of the word or phrase in other sections of the Code*, except when a contrary intent plainly appears." *Adams Cty. Record v. Greater N.D. Ass'n*, 529 N.W.2d 830, 834 (N.D. 1995) (citing N.D.C.C. § 1-01-09) (emphasis added); *accord In re Slinger*, No. 16-30505, 2017 WL 1364969, at *4 n. 3 (D.N.D. Apr. 12, 2017). Although N.D.C.C. § 51-22 does not define "disclose" or "disclosure," the North Dakota Uniform Civil Remedies for Unauthorized Disclosure of Intimate Image Act provides for a clear definition of "'Disclosure' or 'disclose'" which it defines as simply "mean[ing] the transfer, publication, or distribution to another person." N.D.C.C. § 32-49-01(3). Thus, "disclosure" and "disclose" as defined under North Dakota Century Code does not encompass Defendant's attempt to manifest a heighted willful or intentional intent.

Third, the legislative history of S.B. 205, supports the contention that N.D.C.C. § 51-22 was specifically meant to protect an individual's sensitive personal information unless there is expressed written consent. Nowhere in the statute's text or the Senate Bill 2051 discussions did

the North Dakota legislature attempt to insert or even mention an intentional or willful conduct level of disclosure. Senator Melland indicated that:

> what [S.B. 2051] really does is provide a penalty for breach of security for people who hold records under computers and this bill simply says that to release any of the information that is available on those computer records without the written consent of the party whose records they are is [a] punishable civil action.

See Data Processing Information Confidentiality Act, S.B. 2051, 47th Leg., ch. 500, § 1 (approved March 19, 1981).[9] Senator Melland further explained that "the purpose of SB 2051 is to provide confidentiality of personal records stored in people's computers." *Id.* Despite the clear purpose of S.B. 2051 and the legislative intent to protect the confidentiality of personal records from a "breach of security," Defendant now argues that the enforcement of N.D.C.C. § 51-22 would create unintended consequences if it allowed for anything other than an intentional or willful disclosure. (Memo. at 14). The fact that Plaintiffs attempt to hold Defendant liable for negligently maintaining their most highly sensitive personal information would not create "an absurd or ludicrous result or unjust consequences" as Defendant asserts. (*Id.*) Contrary to Defendant's contention, this is the exact type of negligent conduct S.B. 2051 was attempting to address when it provided for a civil penalty for a "breach of security" based on the unauthorized release of an individual's personal records.

Fourth, Defendant turns to the Black's Law Dictionary's definition of "disclosure," (ignoring the term "disclose" used in N.D.C.C. § 51-22-02) which it defines as "[t]he act or process of making known something that was previously unknown; a revelation of facts." (*Id.*) Next, finding no solace in the actual definition of "disclosure" to impute an intentional or willful level

[9] The court can take judicial notice of legislative history when the statutory language is susceptible to competing interpretations to assist in determining legislature's intent. *Florida State Bd. of Admin. v. Green Tree Fin. Corp.*, 270 F.3d 645, 654 (8th Cir. 2001).

of culpability, Defendant then delves to a second level of defining a word, "act," used in the definition "disclosure." Focusing on the word "act" used in the definition of "disclosure," instead of the term "process," Defendant finally reaches its presupposed conclusion that a "[d]isclosure requires an affirmative and voluntary act." (*Id.*) Additionally, Defendant fails to provide the Black's Law Dictionary definition of "disclose" which is defined as "[t]o make (something) known or public; to show (something) after a period of inaccessibility or of being unknown; to reveal." Black's Law Dictionary (11th ed. 2011). The Black's Law Dictionary definition of "disclose" also clearly does not attach a willful or intentional action as Defendant ignores.

Finally, unable to find supporting authority, legislative history, or an imputed willful and intentional definition under North Dakota substantive law to support its manufactured heightened level of culpability under N.D.C.C. § 51-22, Defendant turns to inapplicable Georgia, North Carolina, and New Jersey state privacy law analysis to support its untenable position. (Memo. at 15). Conversely, when the statutory language review becomes one of legislative intent, the "authority from other jurisdictions does not provide any insight into the North Dakota statutory scheme." *Carlson*, 2008 WL 873647, at *9; *accord Mid-Century Ins. Co. v. Fish*, 749 F. Supp. 2d 657, 667 (W.D. Mich. 2010) (recognizing that a federal court's interpretation of state law is not binding). Defendant's attempt to foist inapplicable state laws interpreted by federal courts upon North Dakota statutory interpretation should be disregarded.

Defendant continues to assert that "[d]isclosure is an affirmative act" under North Dakota law, but again fails to provide any binding legal support, other than to rely on the *Anthem* data breach case, which analyzed whether the Georgia Insurance Information and Privacy Act applied in the data breach context. (Memo. at 15 (citing *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 1002–03 (N.D. Cal. 2016) ("*Anthem I*"))). Although the court in the *Anthem I*

determined that the term "disclosure" meant "an active, voluntary decision by the information holder to provide data to an unauthorized third party," it also recognized that the Georgia Supreme Court would review how the terms "disclose" or "disclosure" were defined in other sections of Georgia statutes. *See In re Anthem, Inc. Data Breach Litig*., 162 F. Supp. 3d at 1003. The court in *Anthem II*, further considered other sections of the Georgia IIPA, to determine that it was not intended to "punish negligent, unintentional conduct; it punishes willful, intentional conduct." *In re Anthem, Inc. Data Breach Litig*., No. 15-MD-02617-LHR, 2016 WL 3029783, at *40 (N.D. Cal. May 27, 2016) ("*Anthem II*") (recognizing that Georgia statutory law (IIPA) text clearly draws a distinction between negligent, unintentional acts and willful, intentional acts); s*ee also Fero v. Excellus Health Plan, Inc*., 236 F. Supp. 3d 735, 784 (W.D.N.Y. 2017) (recognizing that both the New Jersey and North Carolina statutory law clearly prohibit intentional disclosure of personal information because both exclude negligence causes of action and specifically state a necessary act "with malice or willful intent to injure any person").

The court in *Fero*, recognized that the Georgia, New Jersey and North Carolina statutes that required "disclosure" also all clearly negated negligence with nearly identical statutory language which specifically required "malice or willful intent." 236 F. Supp. 3d at 784 ("No cause of action in the nature of . . . negligence shall arise against any person for disclosing personal or privileged information in accordance with this act . . . provided, however, this section shall provide no immunity for disclosure or furnishing false information *with malice or willful intent* to injure any person." (emphasis added)). Unlike the state statutes in Georgia, New Jersy and North Caroline, the North Dakota statute does not require an intentional act with malice or willful intent anywhere in the statute.

The statutory definition and inapplicable state law analysis that Defendant goes through to arrive at its unfounded conclusion that a "disclosure" must require "an affirmative and voluntary act" (Memo. at 13–16), is unsupported by the North Dakota statutory text, relevant case law, legislative history, or dictionary definitions. Instead, under N.D.C.C. § 51-22, disclosure does not require an affirmative and voluntary act, but instead, only that a person's records were disclosed without expressed written consent. *See* N.D.C.C. § 51-22-02(1).

Accordingly, Defendant's motion to dismiss Count VI should be denied.

VI. Defendant seeks to create procedural inefficiencies.

Defendant cites no relevant supporting authority for its assertion that Interim Lead Plaintiffs' Counsel should file a separate complaint on behalf of Plaintiff Stock[10] alleging the same facts and the same legal causes of action. Instead, Defendant cites to an inapposite employment litigation case outside the class action context in which new plaintiffs were added to a consolidated complaint, adding additional retaliation claims. (Memo. at 16) (citing *Garnett-Bishop v. N.Y. Cmty Bancorp, Inc*., No 12-CV-2285 (ADS)(ARL), 2014 WL 5822628, at *5 (E.D.N.Y. Nov. 6, 2014) (ruling that even if plaintiffs had sought leave to amend the consolidated complaint, their amendment would be futile). Here, Plaintiffs did not plead any additional legal causes of liability when Plaintiff Stock's claims were included in the consolidated complaint. (*See* CAC at ¶¶ 133–191). Additionally, Defendant claims that Plaintiff Stock asserts "allegations unique to her" which

[10] Defendant identifies information outside the pleadings when it states that it failed to identify "'Samantha Stock' as an individual for whom Defendant held PI or sent a notice of the data incident." (Memo. at 2 n. 1). Defendant's records clearly have a typo related to Plaintiff Stock's last name as evidenced by her September 8, 2023, data breach letter addressed to "Samantha Stack" and a simple investigatory deduction Defendant could have easily made when searching its records for all September 8, 2023, data breach notice letters sent to the small town of Silver Bay, Minnesota (population 1,857). (CAC at ¶ 15).

Defendant will have the opportunity to raise at class certification if she does in fact possess the alleged undisclosed unique attributes that would disqualify her as a class representative.

The Federal Rules of Civil Procedure allow a court to issue any other orders to avoid unnecessary cost or delay if the actions before the court involve common questions of law or fact. Fed. R. Civ. P. Rule 42(a). "Under Rule 42, courts have substantial discretion in questions of consolidation." *Greiner v. Delorme*, Nos. 4:14-cv-39, 3:18-cv-247, 2020 WL 12957751, at *2 (D.N.D. Apr. 23, 2020) (citing *Hall v. Hall*, 138 S. Ct. 1118, 1131 (2018)); *see also E.E.O.C. v. HBE Corp*., 135 F.3d 543, 550–51 (8th Cir. 1998) (stating that claims and issues sharing common aspects of law or fact may be consolidated to avoid unnecessary cost or delay). Indeed, Rule 42(a) is permissive and grants the court broad discretionary powers to order consolidation if it would avoid unnecessary costs or delay. The Court has done just that. (Order, ECF No. 11).[11] Defendant's procedural assertion also clearly ignores Fed. R. Civ. P., Rule 1 which is based on the premise that the rules "should be construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action and proceeding." Fed. R. Civ. P. 1; *accord id.*, Committee Notes (2015) ("[D]iscussions of ways to improve the administration of civil justice regularly include pleas to discourage over-use, misuse, and abuse of procedural tools that increase cost and result in delay.").

Moreover, Defendant does not assert that it has been prejudiced by the addition of Plaintiff Stock to the CAC, instead, Defendant complaint concludes that it was merely procedurally "improper and the new plaintiff should be dismissed." (Memo. at 16). In other words, Defendant requests the Court dismiss Plaintiff Stock and her legal claims because she is alleged to be a

[11] Plaintiffs respectfully request that if the Court is inclined to dismiss Plaintiff Stock's claims as an improper amendment to the CAC, the dismissal be without prejudice so that she may file a separate action alleging the same common questions of law and fact.

procedurally improper plaintiff, and in turn would prefer Plaintiff Stock to file a separate complaint alleging common questions of law and fact, and then Defendant could presumably proceed to file a motion to consolidate the action with the current case pending before the Court. (*See* Order, ECF No. 11) ("If other cases that share common questions of law or fact are filed in this district, any party may move to consolidate those cases with these four consolidate cases.").

Defendant's motion to dismiss Plaintiff Stock and her claims, attempts to create procedural inefficiencies which would result in unnecessary delays and expense.

CONCLUSION

For the foregoing reasons, Defendant's Motion to Dismiss should be denied.

January 29, 2024

/s/ Scott Haider

Scott Haider (ND #07533)
SCHNEIDER LAW FIRM
815 3rd Ave., S.
Fargo, ND 58103
Phone: 701-235-4481
Fax: 701-235-1107
scott@schneiderlawfirm.com

HELLMUTH & JOHNSON PLLC
Nathan D. Prosser
Anne T. Regan
8050 West 78th Street
Edina, MN 55439
Phone: (952) 941-4005
nprosser@hjlawfirm.com
aregan@hjlawfirm.com

GUSTAFSON GLUEK PLLC
Daniel E. Gustafson
David A. Goodwin
Daniel J. Nordin
Joe E. Nelson
Canadian Pacific Plaza
120 South 6th Street, Suite 2600
Minneapolis, MN 55402
Phone: (612) 333-8844
dgustafson@gustafsongluek.com
dgoodwin@gustafsongluek.com
dnordin@gustafsongluek.com
jnelson@gustafsongluek.com

Interim Co-Lead Plaintiffs' Counsel

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
Carl V. Malmstrom
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner*
Philip J. Krzeski*
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612)-336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
Nickolas Hagman*
Alex Lee*
135 S. LaSalle, Suite 3210
Chicago, Il 60603
Phone: (312) 782-4880
Fax: (612)-336-2940
nhagman@caffertyclobes.com
alee@caffertyclobes.com

* Pro Hac Vice Application Forthcoming